

RISK ASSESSMENT / SECURITY & HACKTIVISM

Details on the denial of service attack that targeted Ars Technica

Take a "booter" site survey, earn attacks like ones that targeted Ars, Brian Krebs.

by Sean Gallagher - Mar 18, 2013 9:20 pm UTC

HACKING NETWORKING



Aurich Lawson / Thinkstock

Last week, Security Editor Dan Goodin posted a story about the ["swatting" of security reporter Brian Krebs](#) and the denial of service attack on Krebs' site. Soon after, Ars was targeted by at least one of the individuals behind the Krebs attack. On Friday, at about noon Eastern Daylight Time, a denial of service attack struck our site, making connectivity to Ars problematic for a little less than two hours.

The attack continued to run throughout Friday. At 9pm EDT, when our hosting provider brought down one of the filters that had been put in place to thwart it, it quickly became apparent that the attack was still underway, and the filter was restored. The most aggressive filters were finally removed on Saturday.

At least in part, the offensive used the same attack tool and user credentials that were involved in the denial-of-service (DoS) attack on Krebs On Security, as Krebs himself revealed [in a blog post](#). The attackers used multiple accounts on TwBooter, a "booter" site that provides denial of service attacks as a paid service (ostensibly for security testing purposes), to launch an automated, denial of service attack on Ars. And at least one of those logins was also used to attack Krebs' site.

TwBooter masks all of the complexity of launching attacks against sites. Users of the site can, depending on how much they pay, launch up to three simultaneous automated attacks against sites through a simple Web interface. TwBooter users can even set up multiple accounts and fill up the queue of the service's "attack server."

It doesn't cost much to get in on the ground floor with TwBooter—an account with rights to a single automated attack of up to 60 seconds in length is \$10 for a month. This means you can launch as many 60 second attacks as you want, one at a time, all month long. The "license" to launch up to three attacks at a time of up to two hours duration is \$169 a month—but there's a 20 percent discount if you pay through Liberty Reserve instead of PayPal. There's also a free plan that allows for attacks up to 300 seconds long. That service requires users to pick an attack type from a pull-down menu in a Web form.

PayPal payments for the site are routed to Sebastien Lariviere, a former IT technician for the county government (MRC) of Pierre-De Saurel in Quebec (now operating as Lariviere Security). Lariviere did not respond to e-mails from Ars for comment.

Obviously, sites like TwBooter generate a lot of ill will and are ironically the target of DoS attacks themselves. Like many legitimate and "black hat" sites—such as the site [exposed.su](#), a website that recently posted the personal information of many public figures—TwBooter runs behind the CloudFlare content delivery network as a way of shielding itself from attacks.

TwBooter may not have been the only service used to launch the attacks on Ars and Krebs. "There are dozens of these booter services out there, most of them based on the same source code," Krebs told Ars. But Krebs received a tip pointing to a dump of TwBooter's customer database—openly accessible on the services' website. It's clear the TwBooter site was part of the attack. A snippet from the SQL dumps Krebs provided to Ars show that multiple attacks (including Slowloris, TCP amplification, and SYN flood attacks) were queued up by multiple accounts on the site.

Pick your poison

Some of the attacks served up by TwBooter are targeted at Web servers themselves. For example, HTTP Get and Post attacks attempt to overwhelm the ability of the targeted server to respond by filling up buffer memory with requests. But there were a few attacks thrown at Ars that don't require the massive traffic of a million-PC botnet.

Slowloris, for example, takes a less brute-force approach—it's a [slow HTTP attack](#) that exploits a misconfiguration of the Apache Web server. It sends partial HTTP requests to its intended victim, which forces

[Enlarge](#) / Individual accounts using TwBooter's server can be "licensed" for up to three simultaneous attacks lasting up to two hours, if you can come up with the cash. Free plans can be set up in exchange for filling out a few surveys.

[Enlarge](#) / The Web form for launching attacks from TwBooter's free attack service.

the server to keep the connection open while waiting for the rest. Because it relies on very little traffic to do the job, it doesn't have to be distributed to work. But since it's dependent on the target being an Apache server that hasn't been tweaked against the slow HTTP style attack, it's not very effective against high-volume Web servers (especially sites using NGINX Web servers, like Ars).

Another attack used against Ars was the RUDY, or R-U-Dead-Yet attack, which also uses relatively few packets. Instead of sending partial requests, it sends what seems like an unending HTTP POST, sending a very large value for content-length in the POST request header. That keeps the server waiting for the rest of the POST to come until the length is reached... which never happens.

Other attacks in the "booter" arsenal go after the network connections of the targets themselves. SYN Flood attacks, for example, attempt to overwhelm the target's network connection by creating a huge volume of "half-open" network connections, using the nature of the TCP protocol's "three-way handshake" to use up server resources. The attacker sends SYN, or "synchronize," requests to the target; the target responds with a synchronization acknowledgement (SYN-ACK), which would normally prompt a return acknowledgement (ACK) message from a legitimate user connection. Instead, the attacker never sends ACK packets back, and the target is left with unfinished connections filling up its network buffers until it can't handle any more connections. These packets are usually sent with forged headers (since the attacker never has to actually get the SYN-ACK from the server), so they're difficult to trace and can appear to be more distributed than they actually are.

Another attack type flung at Ars was a UDP-LAG attack. It just uses a large stream of UDP packets in an attempt to overwhelm a target's network connection and knock them offline. UDP-LAG attacks on "booter" services are often used by online gamers who want to slow down the network connections of a competitor. This way, they can camp on their location and kill them while they lag, respawn, and lag some more. Because they use UDP packets, UDP-LAG attacks in large volume can look like DNS amplification attacks—attacks that use responses from DNS servers to spoofed requests that give the address of the target.

Shrugging it off

Fortunately, Ars' hosting provider was able to quickly identify the attacks that were causing the most damage to site availability. Our IT team alerted our provider to the problem at 12:09pm EDT on Friday; the problem was mostly in hand by 1:30pm through the application of traffic filters at the provider's router.

But the fact remains that anyone with some spare change, spare time, and an axe to grind can turn to sites like TwBooter and stage DOS attacks at will—with little fear of retribution. The sites come and go, hiding behind the thin veil of a "terms of service" agreement that asks users, *pretty please*, to not misuse their attack servers. These booters profess that they are for "security professionals only"—yet they do little to track the actual identities of those who use the servers.

Update: Brian Krebs did some further reporting on the TwBooter hacker's identity today. Krebs found the same individual may have been involved in the Krebs swatting, the Ars DoS, and the identify theft executed on *Wired's* Mat Honan last fall. Information about Krebs' findings have been spun out into [an additional post](#).



Sean Gallagher / Sean is Ars Technica's IT Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.
[@thepacketrat](#)